Reading this Template Terms of Reference (ToR)

This template has been drafted for the purpose of providing (new) EU ISAC initiatives with a document that provides a starting point for the development of their own Terms of Reference. It has been drafted by reformulating the terms of reference of an already existing EU ISAC. The template ToR is flexible and can be adjusted depending on the needs of the ISAC being formed, and the sector in which it operates. It is not the only template which can be used for an ISAC but given that it caters for many of the issues which stakeholders may need to consider, it is useful as a reference point, even if a different model is chosen.

The intention of the template is to provide options for tailoring various provisions. Many provisions are presented as "[A/B]" where the sentence can be completed by deleting the non-desired option. For example "~~[~~Simple~~/qualified]~~ majority vote". The template covers key elements of a ToR:

Purpose and objective of ISAC

Chapter 2, setting out the purpose and objectives are quite general, and reflect the needs of an already-formed ISAC. At the initial meetings to discuss the formation of the ISAC, the purpose and objective of the ISAC should be central. The text in this ToR can assist those discussions and can be replaced or amended based on the output of those discussions. The key is to reflect the consensus of the stakeholders seeking to form the ISAC and to reflect the needs of the sector in which they operate.

Membership and representation

This template ToR presupposes that organisations will be members, and that they will be represented at the ISAC by natural persons. Thus, a clear distinction is retained between members and representatives, when setting out their obligations, their interaction with the ISAC, and any possible sanctions.

Governance

The governance approach in this template leans towards a model whereby a Board is elected from the representatives of the members of the ISAC with competence to conduct certain activities. More activities can be added with the consent of the membership (through their representatives). The members gather in plenary through their representatives at General Meetings, but there is also provision for smaller steering/working groups. Other models are possible: there could be a co-chair with a representative of 1 entity per Member State , or some arrangement whereby certain types of stakeholders are ensured representation (e.g. those responsible for infrastructure). This is something for discussion. The crucial issue is to ensure that the board or other governance arrangement ensures adequate representation of the membership and is accountable to the broader membership.

A degree of flexibility is retained in this template in relation to voting, which is something to be discussed by stakeholders forming an ISAC. The main issues to consider is whether decisions are to be taken by simple majority (i.e. 50%), which tends to allow for a more dynamic approach to governance, or a qualified majority (e.g. 2/3^{rds} of votes, or 75%) or even unanimity, which has the advantage of ensuring that any decision is obtained through consensus. It may be desirable that certain decisions require a mere simple majority, but others (which may substantially alter the manner in which the ISAC operates) require a qualified majority or unanimity.

The other issue to be discussed when framing the governance provisions is the quorum. This may depend on the number of members, the assiduity and level of participation. On the one hand, the

quorum is a useful way to ensure that decisions are not taken without the broad consensus (e.g. a 100% vote taken by 20% of the members would not seem to reflect consensus), but having rules on quorum which are too strict could hinder the work of the ISAC (e.g. a requirement to have 80% of members present in order to vote, when the reality of the ISAC in question is that 80% of members are rarely expected attend meetings). Any quorum rules should thus be realistic.

The other issue which may arise in relation to both the question of majority and quorum is whether a differentiation is needed between different members. For example, if a minimum number of private or public sector representatives needs to be present, or if entities in different market positions need to be represented (e.g. those responsible for the network).

Information sharing

In the interests of simplicity and generality, the information sharing rules in this template are those of the traffic light protocol (TLP) as understood by ENISA in relation to ISACs. Those forming the ISAC can assess whether these are appropriate for their situation or may need to be amended.

Sanctions

This template provides for the possibility of the removal or a member or its representatives in the event of a breach of their obligations as set out in the ToR. It provides that the removal requires a vote at a general meeting, and for the right to be heard on the part of the representative/member (in the interests of natural justice). It is unlikely that such sanction provisions will be necessary, and some stakeholders may regard them as being too formal. However, it is also possible that the existence of provisions on sanctions can create trust; as there is a formal procedure in place, members can satisfy themselves that if an issue does arise with a member's conduct which may negatively impact the operation of the ISAC, there is a process to remove them. Conversely, all members know that they cannot be removed capriciously and without the opportunity to present their case.

Independence

It may be that, for certain fledgling ISACs, another organisation already exists in their sector, which has resources or expertise which can help the ISAC pursue its objectives. While this may have advantages, it is also important that it does not threaten the independence of the ISAC itself or give rise to questions regarding transparency or conflict of interest. The best way to ensure this is to describe as clearly as possible the extent of the involvement of this organisation, and to re-state that the ISAC members' primary obligation is to the ISAC itself.

Miscellaneous provisions

Certain miscellaneous provisions may be necessary for some ISACs. The ones in this template, taken largely from the ToR of an existing ISAC, relate to the interaction between the members and the issue of binding other members, or engaging in anti-competitive conduct. It may be that other issues not dealt with in this template arise during early discussions, which do not fit neatly into other sections of the template. In this case, the miscellaneous provisions section may be a useful place to record these.

1. The Terms of Reference

1.1. Document purpose

The purpose of this Terms of Reference (ToR) is to describe the XX-ISAC and to form the membership agreement for the members.

1.2. Scope of this document

In this document the ToR for the XX-ISAC will be described, both for the 'physical' ISAC as well as the virtual (forum).

This Terms of Reference will:

- Define purpose of XX-ISAC;
- Define objectives of XX-ISAC;
- Set out the provisions on membership;
- Set out the provisions on Representatives;
- Describe the governance of XX-ISAC, including participation, information sharing and transparency; and
- Set out the provisions on sanctions.
- Set out a number of miscellaneous provisions concerning the XX-ISAC Member's interactions within XX-ISAC.

1.3. Intended audience

This Terms of Reference is intended to provide information to the following:

- All XX-ISAC members;
- All potential XX-ISAC members.

2. XX-ISAC

2.1. Purpose of XX-ISAC

[The purpose of XX-ISAC should be discussed and decided upon by the initial members. In a broad sense, the purpose of ISACs will be to contribute to better cybersecurity in the given sector, by providing for the sharing of information on threats, vulnerabilities or incidents. Within the EU, participation in an ISAC by certain entities may facilitate their meeting of obligations under the NIS Directive. In a more specific sense, the purpose of the ISAC may vary depending on the level of interaction or sharing of information, and the types of information which it is intended to share, and also the sectoral or geographical scope. The purpose as described below is an example of how this section of the ToR could be described. The text below is inspirational and we strongly encourage ISACs to critically and clearly formulate and define their own purpose.]

The purpose of XX-ISAC to provide a trusted and confidential environment where participants from the [sector] value chain will share information on threats, vulnerabilities and incidents. This can and will be done both by physical and virtual meetings (e.g. a web-based solution, conference calls, etc.). Both the physical and the virtual meetings are important, however the psychical meetings will help to build trust between the members, due to seeing one another etc., so information can and will be shared more openly and willingly.

The mission statement of the XX-ISAC is as follows:

"To improve the cybersecurity and resilience of the European [sector] infrastructure through trust-based security data and information sharing and analysis on threats, vulnerabilities, incidents, solutions and opportunities.

XX-ISAC offers a community of stakeholders to facilitate this proactive data and information sharing and analysis, allowing its members to take their own effective measures."

2.2. Objectives of XX-ISAC

[These need to be defined by the initial stakeholders for their ISAC when setting it up. Many of these objectives will be relevant to most/all ISACs, but there may be some which are specific to certain sectors. It is also an option to order them in terms of priority. This list is of course not exclusive and once again mostly inspirational.]

a) Establishing a trusted environment where information can be shared with those responsible for the protection of [elements of critical infrastructure whose protection is necessary] as an element of the Critical Infrastructure (CI);
b) Supporting the search for answers and solutions to vulnerabilities, which otherwise could be exploited;
c) Preventing attacks on the [elements of critical infrastructure whose protection is necessary] elements of the CI through the development and implementation of 'best practices', 'lessons learned' and Incident Response Plans;
d) Supporting an active community to identify and analyse threats, vulnerabilities and incidents on the unauthorized entrance or manipulation of networks or software supporting the CI;
e) Ensuring membership mutual support and expert-to-expert contact via discussion groups, patching information or Q&As;
f) Enabling public private cooperation in the field of cyber security, related to the [XX] sector.
g) Co-organizing cyber security (awareness) activities for the target group/sector, such as awareness campaigns, thematic sessions or conferences.

3. Membership

3.1 Membership criteria

[Considerations for membership criteria: they should be clear and non-discriminatory. They should seek to include all entities whose involvement is necessary for the effective functioning of the ISAC, and exclusionary criteria should be limited to where necessary (either due to legal prohibition, or the compromising of optimal sharing by other members). In case an entity is excluded from full membership, other forms of membership or participation could be explored, which might enable the resources and expertise of that entity to be made available to the ISAC without compromising one of the reasons why they are excluded from full membership].

a) Membership of the XX-ISAC is open to organizations (public, private or public- private) and academia which comply with the following criteria and whose membership does not compromise the availability, confidentiality and integrity of the XX-ISAC.
    I. Companies operating in Europe as part of the [sector] value chain who would be affected by a (cyber) security incident or could have a vulnerability in the [sector] domain. This includes:
        i. Operators of essential services identified pursuant to Directive (EU) 2016/1148 (NIS Directive);
        ii. Digital services providers identified pursuant to the NIS Directive;
        iii. European and national bodies that are directly or indirectly affected in their objectives by (cyber) security incidents;
    II. Academic institutions and other knowledge institutions (e.g. universities and research institutes) which have knowledge about (cyber) security/incidents of critical infrastructures and are able to analyse information and help creating solutions.
    III. [*ISAC Members to complete*]
    IV. […]
b) An entity can only become a Member if compliant with the following requirements:
    I. It is capable of and committed to delivering identifiable added value;
    II. It endorses the ToR of the XX-ISAC, agreeing to abide by the provisions on membership and governance, and agrees to ensure its Representative's respect for the obligations on representatives;
    III. [It is an EU-based organisation. Non-European organisations *cannot join but can be granted partner status].*
    IV. [Law enforcement agencies or intelligence agencies (or Governmental bodies obliged to report to these)] *[in this template the suggestion is made that these organizations are involved in another manner and cannot join the XX-ISAC as members, due to the informational imbalance, and the potential of their involvement to erode the willingness of Members to share information openly. The XX-ISAC can instead seek to develop partnerships with such agencies, in order to profit from their expertise and knowledge during dedicated sessions, but without compromising the willingness of Members to share information openly.]*
    V. *[Sectoral regulators cannot join from a similar lie of thought, on the basis that their presence may erode the willingness of Members to share information openly and willingly. The XX-ISAC can seek to develop partnerships with such regulators, in order to profit from their expertise and knowledge during*

dedicated sessions, but without compromising the willingness of Members to share information openly.]

3.2 Changing membership criteria

Membership criteria may be changed when compliant with the following steps:

I. A motion for a change of the membership criteria may be submitted by one or more Members. The motion should state the current criterion/criteria, the proposed new criterion/criteria and the reason for the proposal to change;
II. Members (through their Representatives) shall vote on this motion to change one or more membership criteria;
III. When the Members have voted, the Board [or Secretary] shall verify that the entire voting process took place in a legitimate way and everyone's interests have been taken into account in the decision-making;
IV. [The majority of the votes will decide if the membership criteria will be changed. In the event of members voting equally, the XX-ISAC board will play a decisive role based on their previous observations;] or [A qualified majority (2/3rds / 75%) of votes is required in order to change the membership criteria].
V. The staff of the XX-ISAC will have four weeks to change the membership criteria and give notice of this change to all existing members via e-mail or the ISP.

3.3 Admission for membership

a) An interested party can apply for membership of XX-ISAC by requesting an application form (ANNEX XXX). The interested party will fill in this form and explain why they want to participate in XX-ISAC and what their added value will be. When a new Member is accepted by the existing Members, the existing Members will have agreed with the added value that the new member will bring to the XX-ISAC. The delivery of added value is an obligation on each Member. This application for membership must be endorsed by at least one existing Member, prior to being put to a vote. The chairman or his/her staff will send the application form via e-mail to the existing Members ahead of the vote.
b) The admission of a new Member in the XX-ISAC must be approved by a [simple/qualified] majority vote of the existing Members. The existing Members will have four weeks to respond whether they agree with the admission or not. The response needs to be sent back via e-mail to the chairman who keeps track on this process. [Any Member that has an objection to membership of a particular applicant organization may propose a veto. In this case, a final vote will take place among all members, [with a qualified majority being required]. An existing member can only propose a veto if, in its opinion, the admission does not comply with the membership criteria [or there is a defined conflict of interest].
c) If the admission is not accepted, the admission will be discussed during the next General Meeting where existing members can explain why they did not accept the admission. [The chairman or his/her staff will update the applying organization about this decision.]
d) For every admission for membership to the XX-ISAC the organization has to supply personal information (as is listed in ANNEX XXX) for their Representatives to support the trusted and confidential environment of the XX-ISAC, and those Representatives shall be subject to the obligations set out in Chapter 4.2.

3.4 Obligations of Members

[The choice of contributions from members should consider the need for a viable business model, but also the need to ensure that potential members aren't excluded due to cost. It may be appropriate to have a flat fee for all members, or if a higher degree of funding is needed, it may be appropriate for contributions to differ depending on the size and nature of the organisation. Some ISACs choose to operate on in-kind basis only, in which case it is important to manage expectations by clearly defining what kind of in-kind contributions are expected. Choices about these options will translate into obligations].

a) [All members shall pay an annual fee of XXX Euro to assure the self-sustainability of the XX-ISAC.
   Or
   Members shall pay an annual fee, the amount of which depends on its nature and size as an organisation, as prescribed by Annex XXX.]
b) [The Board/Co-chair/Governance body may elect to permit certain organisations to provide 'services in kind' instead of a membership fee. Academia will pay no fees but will offer in-kind contributions, e.g. performing analysis or helping in compliance.]
c) Members of the XX-ISAC must only use the virtual environment created by the XX-ISAC to share online information, start discussions and to ask questions about relevant topics.
d) Each Member shall attend at least [two General Meetings every year] (these meetings shall be physical, unless the circumstances dictate that this is not possible or appropriate). This is to ensure that information can and will be shared among as many member organisations as possible who will benefit from, or are needed for, the right information for the topic at that time.
e) Each Member is obliged to deliver added value in the XX-ISAC.[1]
f) Members shall not undertake any actions that will badly influence or give a bad reputation to the XX-ISAC in any way.
g) All members will have to follow and participate in all XX-ISAC voting processes (when their vote is needed), according to the instructions provided by the staff.
h) Members will ensure that their Representatives abide by the obligations on Representatives, as set out in Chapter 4.2.

3.5 Termination of membership

I. An organisation shall remain a Member of XX-ISAC until:
(a) its membership of XX-ISAC has been revoked in accordance with the procedure set down in Chapter 6; or
(b) it notifies the [Board/Co-chair/Governance body] that it wishes to withdraw from XX-ISAC.

II. In the event that the Member which they represent wishes to withdraw from XX-ISAC, it will commit to respecting the classification of any information that has been shared with it prior to the withdrawal (this includes ensuring that its Representatives respect the classification of any information shared with them prior to withdrawal).

III. Each Member shall use information received from a withdrawing Member during its membership and which the disclosing party expressly stated to be confidential or the confidential nature of which can be assumed on the basis of the circumstances of its disclosure solely for the purposes for which it was provided, treat it in the same way as their own

[1] What constitutes added value could also be defined somewhere in the ToR.

business secrets and not make it available to third parties. This obligation is notwithstanding the following exceptions:

i. The information was in the receiving party's possession without an obligation to confidentiality prior to receipt from the disclosing party;
ii. The information was at the time of disclosure already in the public domain or subsequently becomes available to the public through no breach of this confidentiality obligation by the receiving party;
iii. The information has been lawfully obtained by the receiving party from a third party without an obligation to confidentiality, provided such third party is not, to the receiving party's knowledge, in breach of any obligation to confidentiality relating to such information;
iv. The information is shown to have been developed independently by the receiving party or its affiliates without reliance on the disclosing party's confidential information; or
v. The information is approved for release by written agreement of the disclosing party.

The member seeking the benefit of such exception shall bear the burden of proving its existence. The receiving party may disclose confidential information of the disclosing party if the receiving party is required to do so by any ruling of a governmental or regulatory authority or court or by mandatory law, provided that written notice of such ruling is given without undue delay to the disclosing party so as to give the disclosing party an opportunity to intervene and provided further that the receiving party uses reasonable efforts to obtain assurance that the confidential information will be treated confidentially.

4. Representatives

4.1 Representative criteria

[The representative criteria should reflect the needs of the ISAC. It is important to ensure sufficient representation of all members, but it may also be important to limit the level of representation of certain members, if this might lead to the perception that they exercise too much control over the direction of the ISAC]

a) Each Member shall be represented by a minimum of one and a maximum of X Representatives. The XX-ISAC will maintain a complete and actual list. [To be amended to reflect the nature of the ISAC]
b) Only Representatives may attend physical meetings of the XX-ISAC. It is not possible for a Member to send another individual in place of a duly nominated Representative. Members can, however, replace one of their two Representatives in accordance with 4.1.(c).
c) A Member can replace a Representative. The proposed new Representative must complete the Representative Application Form (RAF)[2], indicating why they wish to participate in the XX-ISAC and what their added value will be. The RAF must be submitted by the Member to all Members. The Members will have two weeks to send a response to the [chairman], indicating whether they wish to exercise their veto in relation to the proposed representative. Should no Member exercise their veto, the [chairman] shall notify all Members of the Representative's appointment. [Should a Member exercise their veto, a vote on the admission of the Representative shall be held at the next General Meeting.] The vote shall be passed by a simple majority (50%) [or the vote shall be passed by qualified majority (2/3rds / 75%)].

[2] Annex XXX

4.2 Obligations on Representatives

The Representatives of the Members exercise their roles subject to the following obligations. Each Member shall be responsible for adherence by its Representatives to these obligations.

a) Each Representative will have a profile that reasonably supports the objectives of XX-ISAC.
b) Each Representative shall comply with these terms of reference and will do endeavour to maintain the trusted and confidential environment of the XX-ISAC.
c) Each Representative shall maintain the confidentiality and integrity of the information shared within the XX-ISAC, and shall apply the rules for participation and information sharing set out in Chapter 5.5 and 5.6 respectively.
d) Each Representative may share information and make decisions necessary to achieve objectives of the XX-ISAC, on behalf of the Member they represent.

5. Governance

5.1 XX-ISAC Board/Co-chair/Governance body

a) The XX-ISAC board will be formed of [5] Representatives, so there is always a majority when decisions need to be made. Only one Representative from each Member can join the XX-ISAC Board. Each Representative wishing to join this [Board] shall:
   I. Announce to every participating Member (via e-mail or the ISP) their desire to join the XX-ISAC Board and give his/her reason(s);
   II. During the next General Meeting, the Members will vote, via their Representatives, on the proposed change to the Board composition;
   III. If there is only 1 candidate for each available position on the Board, their selection will be by [simple majority (50%)/qualified majority (2/3rds/75%)] of the Representatives present [provided that the quorum is met].
   IV. If there are more candidates than available positions on the Board, the candidate with the most votes will be selected for the first available position, the candidate with the second most votes for the second position etc, until all the positions are filled.

b) This XX-ISAC board will have an official role in core governmental decisions and acts, e.g. the official recognition of new members.

c) The XX-ISAC Board will play a decisive role (if needed) for the formation of a new working group or in casting deciding votes.

d) The XX-ISAC Board will also monitor the voting process to check if it is done in a legitimate way and to make sure that everyone's interests have been taken into account in the decision-making. [From a Governance perspective, could have a separate Secretary, who monitors this, and who does not have a vote].

e) More XX-ISAC Board activities may be added when compliant with the following steps:
   I. The XX-ISAC Board gives notice to all Members of a new activity they want to perform;
   II. All Members vote if the XX-ISAC Board may perform that activity;
   III. The vote shall be decided by [simple majority (50%)/qualified majority (2/3rds/75%)] of the Representatives present, [provided that the quorum is met].

f) If a XX-ISAC Board member wishes to withdraw from the XX-ISAC Board, they shall give notice and, if required, an explanation to all Members. With the withdrawal of that representative, a new XX-ISAC Board member has to be appointed in accordance with the procedure set out in paragraph a), so that the XX-ISAC Board again consists of 5 Representatives.

5.2 Board Meetings

a) A Board Member shall be elected by the [Board Members/ISAC Representatives] as rotating chairman by for a [fixed period of 2 years].[3]

b) The meeting quorum for the Board Meetings will be [5 (i.e. 100%)].

[3] There could also be a provision for the appointment of the Secretary, who could have a degree of independence from the other Board Members. The Secretary could be a sixth member, with a non-voting role (meaning there would still be an uneven number of voting board members). The advantage would be a degree of impartiality, in the recording of minutes, and the secretary could have a role in ensuring the integrity of the voting process etc.

c) Any decisions that will be made will be by simple majority of the votes. The decision making will take place either during meetings or via e.g. e-mail, depending on the preferences of the existing Board Members.

5.3 General Meetings

a) General Meetings will be held at least [once/twice] per year.
b) [1/2] Representative(s) of each Member will be entitled to vote on motions proposed at General Meetings.
c) [Motions shall be passed by simple majority (50%)] or [Motions shall be passed by simple majority (50%) except for changes in membership criteria or making additions to the Board's activities, which requires a qualified majority (2/3rds / 75%)].
d) In the event that a vote is tied, the XX-ISAC board will cast the decisive vote.
e) Meeting agenda will be provided by the [Secretary[4] (or someone from the staff of the XX-ISAC).]
f) The minutes of every meeting will be taken by the Secretary (or someone from the staff of the XX-ISAC).
g) General Meetings will last a minimum of one day at [either the premises of a member organisation or a public venue such as a hotel or a conference centre/specify fixed location]. At each General Meeting members will be invited to host the next meeting. Should physical meetings not be possible for health or other reasons, the meetings may be held virtually.
h) Member organizations shall attend at least [two physical meetings per year].
i) Only Representatives of Members of XX-ISAC can participate in the (physical and virtual) meetings. An external expert participant (e.g. to present a certain topic which is relevant for all the members or to present a topic of interest in a restricted workshop) can be proposed by any member, but it is subject to approval of every member of that group. This means that an external person can only participate in general meetings (with all the Representatives) if a Representative from each Member approves. In the workgroups an external can participate if every member of that workgroup approves.

[4] See Ch 5.1: The ToR would need to provide for the election of the Secretary.

5.4 Steering/Working Group Meetings

a) Members with the same focus area may form workgroups within the XX- ISAC as long as they do not forget the main purpose of the XX-ISAC: a cross chain collaboration. Within these workgroups information about specific topics is more easily shared among peers. Meetings of these workgroups are hosted on their own initiative.
b) For the work/steering group meetings, the members of that group will decide how often they will meet per year and when they need to be present. If a member of a work/steering group does not comply with the agreements of that work/steering group, the other members of that group may decide, by majority of votes, to remove that member from that work/steering group.

5.5 Rules of Participation

a) Any discussion in meetings and views expressed or implied in such discussion or associated documents are without prejudice to and shall not limit the discretion of any of the members of the XX-ISAC with regard to decisions of any European or national organization. Equally views expressed by participants during the meetings will not be treated as the formal position of the organization they are representing, and will not prejudice consultation responses.

b) During the XX-ISAC meetings sensitive information will be shared. All agenda meetings will be assigned an information sharing level of WHITE, GREEN, AMBER or RED.

c) When needed, meetings (with all XX-ISAC members) will operate on the basis of a bipartite structure of two sessions. The first of these sessions will deal with issues that are classified at the WHITE information sharing level and are open to external participants. The second session will deal with issues that are classified at the GREEN, AMBER or RED information sharing levels on account of the security and risk implications associated with wider disclosure of such information. These meetings will only be accessible to the existing Members of the XX-ISAC.

d) Each Member will be asked to undertake in writing to abide by the confidentiality and disclosure obligations, in relation to each information sharing level, by signing the confidentiality and disclosure agreement at Annex XXX of this ToR. The signing of this agreement will happen once at the beginning of the membership and shall be maintained at all times.

5.6 Information sharing

Sensitive information will be exchanged during the closed part of the XX-ISAC meeting. Every representative must classify the information provided by him/her with one of the four colour classifications. This classification is his/her interpretation of how this information has to be treated by the other representatives.

a) The four colour classifications are:[5]

[5] Based on the current ENISA understanding https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/considerations-on-the-traffic-light-protocol

RED	Not for disclosure, restricted to participants only. Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.	Information shared with people in a meeting; direct email.
AMBER	Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.	Sharing of Indicators of Compromise (IoCs) to an organisation's CSIRT. These could be forwarded to the SOC for further action.
GREEN	Limited disclosure, restricted to the community. Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share	Sharing of a malware analysis with a specific industry sector.

a) It is the responsibility of all representatives to respect and act in accordance with the XX-ISAC colour classifications.
b) It is the responsibility of the representative who shares the information to label the information with a colour classification. In the event that there is no colour classification the information itself will be labelled [AMBER] and the identity of the sharing representative is labelled [RED].
c) A representative has to be sure about the colour label of the information. When in doubt he/she will first assure him/herself of the colour label before handling the information.
d) [It is possible to share information with the colour label RED or AMBER anonymously. The information has to be delivered to the chairman of the XX-ISAC, who will then share this information within the XX- ISAC.]
e) Members of the XX-ISAC must only use the virtual environment created by the XX-ISAC to share online information, start discussions and to ask questions about topics. This only applies to XX-ISAC related communication. The platform must not be used for the advertisement of companies, etc., but only for above mentioned activities. All information being shared on this platform must also have a colour classification.
f) The XX- ISAC is not an instrument to report criminal activities to law enforcement agencies. Reporting of such activities should be done outside the XX- ISAC.
g) In the information shared within the XX- ISAC all personal information should be anonymised. Neither the identity nor the connection of the speaker(s) shall be revealed (Chatham House Rules).
h) If another XX-ISAC representative, upon receipt of the information, has a different opinion on the classification of the shared information they can express their opinion to the other representatives of the XX-ISAC, provided that doing so does not require treating the information in a manner prohibited by the colour classification of the person

providing it. The XX-ISAC board has a final saying in changing the classification of the shared information.

i) [Claims for damages against another member in relation to its activities within XX-ISAC shall be excluded, irrespective of their legal grounds and to the greatest extent permitted by law. In particular, no member shall be liable, whether for negligence, breach of contract, tort, misrepresentation or otherwise, for any indirect, incidental or consequential loss or damage, howsoever arising, lost time, loss of revenue or profit, loss of production, loss of interest, loss of power, interruption of operations or loss of use, cost of capital, cost of purchased or replacement power, goodwill, anticipated savings, loss of information or data or damages based on third party contracts, in each case even if advised of the possibility of such loss or damage.]

5.7 Transparency

a) The XX- ISAC may decide to publish XX- ISAC information, including the schedule of meetings dates, agendas and other items such as minutes or papers. To publish information of the XX-ISAC all members will have to agree with this decision. Any member who does not agree with this decision will have to make his/her objection clear to the rest of the members. The members will then vote on whether or not publish the information and the decision will be dependent on the majority of the votes.
b) Agendas will include GREEN information sharing level items. Minutes of meetings will include AMBER information sharing level items, as often these minutes will contain more information about a specific incident and the lessons learned. For papers the content will determine which information sharing level it will be given. This has to be decided by the members.
c) If a closed user group within the web platform is established, GREEN and AMBER classified information can be published on the web platform. Only the closed user group members shall have access to this shared information and the information owner should have the ability to define the group with whom he or she wants to share the information.

6. Sanctions

[These kinds of sanctions are unlikely to be needed very often. They could also be phrased more restrictively, requiring "breach of multiple obligations" or "serious breach". For example, breach of confidentiality is naturally more serious than merely not attending a couple of General Meetings. Similarly, it could be set up so that each motion needs to be seconded by another member.]

6.1 Removal of Member

A Member may have its membership of XX- ISAC revoked if the Member is shown to have failed to abide by one or more of its obligations as set down in Chapter 3.4 of these terms of reference.

6.2 Removal of Representative

A Representative can be removed as a Representative if they have been shown to have failed to abide by the any of their obligations as per Chapter 4.2 of these terms of reference.

6.3 Sanction procedure

[It is important to include something on procedure, and in particular the requirement of natural justice that the party being sanctioned have a right to be heard.]

a) Any Member of XX-ISAC may propose (through its Representative(s)) a motion to terminate another Member's membership, in the event of a breach of the obligations set out in Chapter 3.4. This motion may also be proposed by the Board *ex officio*. Any such motion shall include the particulars of the claim:
   - The obligation which is alleged to have been breached;
   - Any evidence of the breach; and
   - The damage or potential damage caused by the breach.

b) Any Member of XX-ISAC may propose (through its Representative(s)) a motion to remove a Representative, in the event of a breach of the obligations set out in Chapter 4.2. This motion may also be proposed by the Board ex officio. Any such motion shall include the particulars of the claim:
   - The obligation which is alleged to have been breached;
   - Any evidence of the breach; and
   - The damage or potential damage caused by the breach.

c) The Member or Representative shall be removed by means of a vote at a General Meeting. Removal shall require [simple majority/qualified majority].

d) The Member whose membership it is proposed to terminate or the Representative whose removal is proposed shall have the opportunity to address the Members at the General Meeting prior to the vote on termination or removal.

7. Independence of XX-ISAC

[It may be that the ISAC collaborates with certain other organisations in the sector. Certain members of the ISAC may also belong to that organisation. While the collaboration may bring benefits to the ISAC, in terms of resources or expertise, in the interests of transparency, the interaction between the ISAC and that organisation should be clearly defined. This is particularly the case if not all members of the ISAC are members of that organisation. The members of the ISAC should commit to the independence of XX-ISAC, and the avoidance of conflicts of interest. No model provision is drafted here, as it requires an appreciation of the specific situation of that ISAC, and the sector in which it finds itself].

8. Miscellaneous provisions

a) Nothing in this ToR shall be construed to grant any Member any right to make a commitment of any kind for or on behalf of another Member without prior written consent of that other Member. No member has the authority to bind, act on behalf of or represent any other Member. No Member shall (by their acts or omissions) behave in a manner that could reasonably cause others to believe that it has authority to act on behalf of another Member beyond the authority expressly granted herein.

b) [The Members are independent organization, bound to each other only as provided for herein. Neither this ToR nor any other document or any action taken by the Members is intended to form a partnership, association, joint venture, or other co-operative enterprise.] [This may need to be amended depending on the legal form of any entity established].

c) Members will not have any form of exclusivity under this ToR. All members will remain absolutely free and independent in their business behaviour and decisions. Any member at any time is allowed to work on similar topics and projects.

d) No licenses or any other rights regarding intellectual property rights such as, but not limited to, patents, utility models, trademarks or tradenames, are either granted or conveyed, nor does this ToR constitute any obligation on a Member to grant or convey such rights

e) It is each Member's policy to comply strictly with the European competition law and all other applicable competition/antitrust rules and regulations (hereinafter referred to as "Competition Law"). Any activities of the Members within the context of the XX-ISAC which infringe Competition Law would be seriously detrimental to the interest of the Members. The Members undertake to ensure that all of their Representatives, employees and agents involved in the XX-ISAC understand and appreciate the importance of complying with Competition Law and that appropriate and effective sanctions for breaches of Competition Law are spelt out. The Members agree that they will at all times strictly adhere to all applicable laws and regulations, especially but not limited to Competition Law which prohibits the exchange of competitively sensitive information and/or business secrets including by way of examples information on prices, costs and demand structure, bidding strategy, marketing plans etc.

Annex I

Annex II